



HAL
open science

Resilient and Robust Strategies for Swarming Ad-hoc Networks

Evelyne Akopyan, Emmanuel Lochin, Riadh Dhaou, Bernard Pontet, Jacques Sombrin

► **To cite this version:**

Evelyne Akopyan, Emmanuel Lochin, Riadh Dhaou, Bernard Pontet, Jacques Sombrin. Resilient and Robust Strategies for Swarming Ad-hoc Networks. 2024. hal-04497425

HAL Id: hal-04497425

<https://hal.science/hal-04497425>

Preprint submitted on 10 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Resilient and Robust Strategies for Swarming Ad-hoc Networks

Evelyne Akopyan^{a,c,*}, Emmanuel Lochin^b, Riadh Dhaou^c, Bernard Pontet^d,
Jacques Sombrin^a

^a*TéSA, Toulouse, France*

^b*Fédération ENAC ISAE-SUPAERO ONERA, Université de Toulouse, France.*

^c*IRIT, Université de Toulouse, CNRS, Toulouse INP, France*

^d*CNES, Toulouse, France*

Abstract

We investigate a set of methods aimed at enhancing the resilience and robustness of a mobile communication network, with a focus on a case involving a nanosatellite swarm network. The proposed method focuses on graph division techniques, aiming to recover from impairments while preserving the primary function or mission of the mobile network. By examining the effects of exploration and random selection algorithms on network robustness and resilience, our findings indicate that fair graph division consistently strengthens system robustness by reducing the number of packets to transmit, regardless of the algorithm employed. Additionally, our analysis highlights the superior performance of exploration algorithms, such as MIRW, in enhancing robustness and resilience.

Keywords: Mobile Ad-hoc Networks, Architecture, Robustness, Resilience, Graph Division

*Corresponding author.

Email addresses: evelyne.akopyan@tesa.prd.fr (Evelyne Akopyan),
emmanuel.lochin@enac.fr (Emmanuel Lochin), riadh.dhaou@irit.fr (Riadh Dhaou),
bernard.pontet@cnes.fr (Bernard Pontet), jacques.sombrin@tesa.prd.fr (Jacques Sombrin)

1. Introduction

Enhancing the robustness and resilience of complex systems and ad hoc networks has been a focal area of research for numerous years. System robustness is its ability to withstand internal and external faults. For instance, a drone fleet is deemed robust if it incorporates an energy management mechanism that allows for reduced energy consumption, extends its lifespan, and minimizes the risk of failure due to energy depletion (Alyassi et al. (2023)). On the other hand, resilience characterizes a system's ability to maintain satisfactory functionality despite faults. Cellular networks demonstrate resilience by deploying redundant equipment to address network faults (Rak and Hutchison (2020)). While adding redundancy is a common strategy to enhance resilience, ad hoc networks, lacking infrastructure, cannot rely on external equipment for fault tolerance improvement. Consequently, considering robustness and resilience is crucial during the design of these systems.

This study examines a scenario involving a swarm of nanosatellites in orbit around the Moon, functioning as a distributed radio telescope in outer space (Cecconi et al. (2018)). This system operates as a Mobile Ad-hoc Network (MANET), and configuring it as a space observatory poses communication challenges. As mentioned earlier, the network lacks infrastructure and relies exclusively on wireless Inter-Satellite Links (ISL), with nodes serving as sources, destinations, and routers. In addition, the system must operate distributedly: unlike conventional observation telescopes, which carry one or more measuring devices on a single satellite, a swarm of nanosatellites comprises a single instrument spread across multiple satellites. The distributed nature of this system imposes a significant constraint on the data transmission model, in addition to the absence of infrastructure. In this case study, each node is required to share its data with all other nodes in a manner that resembles any-to-any communication. This data-sharing process is essential for the space observatory to generate a comprehensive image of space observation, which is subsequently transmitted to a base station on Earth.

Nevertheless, the data generated from space observations can be extensive, reaching several gigabits per nanosatellite. The simultaneous transmission of these data packets may result in Inter-Satellite Link (ISL) congestion, potentially leading to packet loss. Each lost packet diminishes the accuracy of the global image, resulting in reduced information transmitted to the base station. Moreover, data transmission poses an energy challenge on the nanosatellite scale. The central nanosatellites within the swarm are

more prone to transmitting a higher volume of packets, depleting their energy more rapidly and causing a subsequent decline in accuracy for the global image. Consequently, a distributed MANET must distribute the data load among each network node equitably. The authors proposed an approach based on a fair graph division of the swarm to balance the network load among nanosatellites, as discussed in Akopyan et al. (2023). Dividing the swarm into multiple groups of nanosatellites significantly mitigates the overall energy consumption of the swarm.

This work’s primary contribution lies in emphasizing the beneficial influence of fair graph division on the robustness and resilience of a distributed MANET, building upon our prior investigations. We introduce a methodology for evaluating robustness and resilience levels before and after graph division, shedding light on any positive or negative effects that graph division may impose on the network’s original robustness and resilience. Enhancing these levels is crucial for improving the system’s fault tolerance and ensuring the proper functioning of the communication scheme. Our findings reveal that fair graph division significantly enhances the system’s robustness, and while specific resilience metrics may experience improvement, it comes at the cost of others.

The rest of the paper is organized as follows: Sec. 2 introduces the graph division mechanism and the division algorithms that will be evaluated. The methodology for assessing robustness and resilience levels in a distributed MANET is presented in Sec. 3. The impact analysis of graph division and the results on the nanosatellite swarm are detailed in Sec. 4. Finally, Sec. 5 presents a literature review of the related work, and Sec. 6 summarizes our study and discusses future research on the subject.

2. Graph division

The main objective of this paper is to highlight the importance of fair graph division for robustness and resilience improvement in MANETs. Graph division is a mechanism that assigns each vertex of the graph to a vertex set called group. Note that the edges remain unchanged; therefore, the groups are still connected with each other and not physically separated. Graph division is a particularly interesting solution for reducing the number of routed packets in MANETs, in the same way that graph clustering helps reduce the number of routed packets in Wireless Sensor Networks (Daanoune et al. (2021)). Graph division has a different purpose from graph clustering: the

core mechanism of graph division is to obtain groups that are similar to the original graph, whereas the core mechanism of graph clustering is to obtain groups such that the vertices within a given group are similar to each other.

We talk about fair graph division when the obtained groups are similar to the original graph and similar to each other: the group size is a straightforward fairness metric, but other metrics can be chosen. The evaluation of fairness in graph division has been thoroughly studied by the authors in a previous paper (Akopyan et al. (2023)).

2.1. Notations and metrics adaptation

Ad hoc networks can be efficiently represented by graphs (Rajan et al. (2008)). Throughout this paper, we model any MANET as a temporal graph $G_t = (V_t(G), E_t(G))$, or simply $G_t = (V_t, E_t)$, with a vertex set V_t representing, for example, sensors, vehicles, or satellites, and an edge set E_t representing communication links (Robinson et al. (2019)). For simplicity, we assume that the communications are performed over symmetrical duplex links, which makes G_t an undirected graph. We also assume that the number of vertices is constant over time, unless stated otherwise.

We consider a MANET scenario in which each member of the network needs to share its data packet (*e.g.* atmospheric records or interferometry measurements) with all the other members, and then combine the data to obtain a global cross-correlation matrix of data collected by the network. This means that each member of the network should communicate with the others. Mathematically speaking, we denote N_G as the total number of vertex pairs that need to communicate in an undivided graph G , defined as follows:

$$N_G = \frac{|V_t|(|V_t| - 1)}{2} = \frac{n(n - 1)}{2} \quad (1)$$

The number of vertex pairs is constant over time because it depends only on the number of vertices in the graph. However, this number would be time dependent if we assumed that the number of vertices was not constant over time.

The robustness and resilience metrics described in Sec. 3 depend on the number of vertex pairs N_G in the graph. However, after performing graph division, the number of source-destination pairs is altered, because the vertices only need to communicate with the vertices of the same group. By limiting data transmission to intra-group transmissions only, each group computes

a partial cross-correlation data matrix. Once all partial matrices are computed, they are shared among the groups and recomputed locally with the additional data to finally obtain the global cross-correlation data matrix.

We denote $G_t^* = (V_t^*, E_t)$ the graph obtained after graph division. The edge set remains unchanged, but the vertices are assigned to x groups in V_t^* :

$$V_t^* = \{V_t^0, V_t^1, \dots, V_t^{x-1}\} \text{ and } \bigcup_{i < x} V_t^i = V_t$$

Moreover, the number of vertex pairs in the divided graph G^* becomes:

$$N_G^* = \sum_{i < x} \frac{|V^i|(|V^i| - 1)}{2} + x(x - 1)$$

where the sum represents the number of intra-group transmissions, and the product represents the number of inter-group transmissions. Because the latter is usually negligible compared with the first, we can simplify the formula to be:

$$N_G^* = \sum_{i < x} \frac{|V^i|(|V^i| - 1)}{2} \tag{2}$$

Thus, the robustness and resilience metrics defined in Sec. 3 are to be adapted to consider only the new source-destination pairs, and not the entire graph.

2.2. Graph division algorithms

Graph division algorithms are often inspired by sampling algorithms. We focus on two main families of algorithms: random selection algorithms and exploration algorithms.

Random selection algorithms are based on the random selection of vertices and/or edges to create a graph sample. In graph division, a random selection algorithm randomly assigns a vertex and/or edge to a group. We choose to work with the Random Node Division algorithm (RND), which performs random selection on vertices only. We decided not to work with edge-related algorithms such as Random Edge Division (RED) because our graph is not guaranteed to be connected; hence, some vertices might never be assigned to any group.

Exploration algorithms are based on neighborhood discovery of a vertex to select the members of a given group. The choice among the neighborhood

can be random, or have a certain probability depending on the characteristics of the vertex. A simple example of exploration algorithms is those based on random walks. We choose to work with the Multiple Independent Random Walks algorithm (MIRW), which, as the name suggests, runs several random walks in parallel in a graph. The particularity of MIRW is that it a random jump in the graph whenever a random walk is stuck (*i.e.*, there are no more free vertices in the neighborhood), to continue the random walk elsewhere in the graph: this mechanism ensures that each vertex in the graph belongs to a group by the end of the division process. Another example of an exploration algorithm is the Forest Fire Division algorithm (FFD), which selects each vertex in a neighborhood with a given probability p . Similarly, FFD performs a random jump in the graph if there are no more available vertices in a neighborhood.

3. Assessment of the robustness and resilience levels

We propose a graph theory-based methodology, applicable to divided and undivided graphs, to assess the levels of robustness and resilience in a network. In this section, we introduce six graph theory metrics that are used to characterize the levels of robustness and resilience.

3.1. Definition of robustness metrics

We focus on three metrics to evaluate the level of robustness of the network: the flow robustness, routing cost and network efficiency. These metrics have been chosen because, when combined, they accurately describe the dynamics of packet transmission in a network.

Flow robustness, denoted $F_t(G)$: the flow robustness of a divided or undivided graph estimates the proportion of the graph that can be reached by a packet through multi-hop. In graph theory terms, the flow robustness of a graph G at time t is the proportion of vertex pairs in G_t connected by a path, and is defined as:

$$F_t(G) = \frac{N_G(t)}{N_G} \quad (3)$$

where N_G is the number of vertex pairs in the graph defined by Eq. 1 (respectively Eq. 2 for a divided graph), and $N_G(t)$ is the number of pairs effectively connected by a path at time t . When the flow robustness equals one, the graph is connected, *i.e.*, each vertex can reach any other vertex in

the graph. Otherwise, the graph is disconnected, so the packets cannot be spread across the entire graph.

Routing cost, denoted $R_t(G)$: the routing cost is the total number of packets to be transmitted through the network to reach all the destination vertices from all the source vertices. We consider a unicast routing strategy for our scenario and assume that the packets always take the shortest path between the source and destination vertices. In this study, as described in Sec. 2.1, all vertices should share their data packets with all other vertices of the network. This means that the vertices in the graph act as sources and destinations. The routing cost of a graph G at time t can be simply defined as:

$$R_t(G) = \sum_{u,v \in V_t^2} d(u,v) \quad (4)$$

where $d(u,v)$ is the shortest path length between the vertices u and v , also called the distance between u and v . The routing cost must be as small as possible because any node in a MANET consumes energy when transmitting a packet. Thus, by transmitting fewer packets in the network, the nodes save more energy and can last longer.

Network efficiency, denoted $\Theta_t(G)$: the network efficiency is a coefficient between 0 and 1 that characterizes the distances between each vertex pair in the graph. If the distances are globally short, *i.e.*, the network efficiency is high, then the packets will need to perform fewer hops and thus be retransmitted less often, eventually saving energy for the nodes of the network. To evaluate the network efficiency, we first compute the pair efficiency for each vertex pair in G_t , denoted $\theta(u,v)$:

$$\theta(u,v) = \frac{1}{d(u,v)}$$

The pair efficiency of vertices u and v equals 0 if there is no path connecting these vertices. The network efficiency of a graph G at time t is then simply defined as the average pair efficiency in G_t :

$$\Theta_t(G) = \frac{1}{2N_G} \sum_{u,v \in V_t^2, u \neq v} \theta(u,v) \quad (5)$$

The network efficiency tends to 1 if most vertex pairs are connected by very short paths, and it tends to 0 if several vertex pairs are not connected

by a path and/or the distances are very large.

3.2. Resilience

As stated in Sec. 5.2, the resilience can be characterized by various metrics. We propose the following three metrics to evaluate the level of resilience in the network: path redundancy, path disparity, and node criticality. We selected these metrics because they thoroughly evaluate the reliability of the paths taken by the packets.

Path redundancy, denoted $\Psi_t(G)$: the path redundancy is a measure of the number of alternative paths in the graph. A path is considered an alternative if it passes through at least one vertex different from the reference path. A great path redundancy is proof of a strong level of resilience because the packets can be routed from source to destination through different vertices if a vertex goes down. Path redundancy is defined as the average number of alternative paths between each two vertices in G_t :

$$\Psi_t(G) = \frac{1}{2N_G} \sum_{u,v \in V_t^2} |P_{uv}| \quad (6)$$

where P_{uv} is the set of paths connecting vertices u and v . If there is no path between vertices u and v , the path redundancy of this pair equals 0.

Path disparity, denoted $\Delta_t(G)$: the path disparity is complementary to path redundancy. It is a measure of the difference between the alternative paths, *i.e.*, the number of different edges composing the paths. A high path disparity ensures that in the presence of a fault on a path, a packet can transit on a completely separate path and hence not be impacted by the fault. We first compute, for each vertex pair, the proportion of different edges between the alternative paths available between the two vertices, which is called pair disparity:

$$\delta(u, v) = \frac{1}{2|P_{uv}|} \sum_{p_i, p_j \in P_{uv}^2} \frac{|p_i(u, v) \oplus p_j(u, v)|}{d(u, v)}$$

where the numerator represents the number of distinct edges between the two alternative paths p_i and p_j . The pair disparity is maximal if the paths are edge-disjoint, *i.e.*, they share no common edge, and is minimal if the paths are identical, or if there is at most one path between two vertices. Fig. 1 illustrates the computation of pair disparity. The path disparity of a graph G at time t is then easily derived as the average pair disparity of the graph:

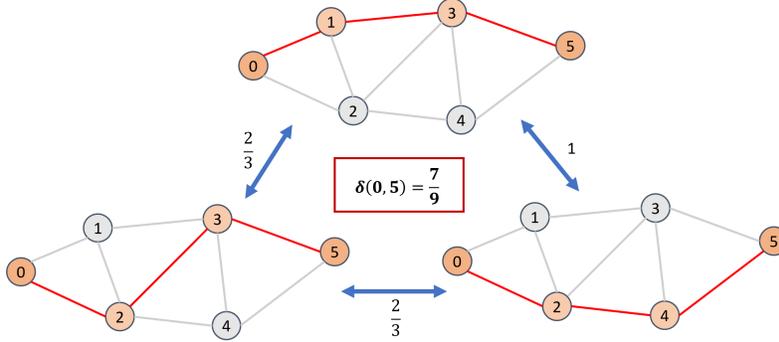


Figure 1: Illustration of pair disparity computation: the pair disparity between vertices 0 and 5 equals $\frac{7}{9}$, or approximately 0.78.

$$\Delta_t(G) = \frac{1}{2N_G} \sum_{u,v \in V_t^2} \delta(u,v) \quad (7)$$

Node criticality: the node criticality is an indicator of the presence and number of critical vertices in a graph. Node criticality is usually based on a centrality measure of the vertices, such as degree centrality or betweenness centrality (Liu et al. (2019)). We choose the normalized betweenness centrality as our criticality measure, defined for a vertex i as follows:

$$BC_t(i) = \frac{1}{2N_G} \sum_{u,v \in V_t^2} \frac{|P_{uv}(i)|}{|P_{uv}|} \quad (8)$$

where $P_{uv}(i)$ is the set of paths from u to v passing through vertex i . The distribution of betweenness centrality values is sufficient to describe node criticality; however, the analysis of the number of extreme values can be a great addition to grasp the dynamics of the graph. As such, we define the critical set $C_t(G)$ of a graph as the subset of vertices whose betweenness centrality is higher than the threshold value ϵ at a given time t :

$$C_t(G) = \{i \in V_t \mid BC_t(i) \geq \epsilon\} \quad (9)$$

By definition, the critical set contains the most critical vertices of a graph, *i.e.*, the vertices that are the most vulnerable to faults. A resilient network tends to have the smallest critical set possible.

To summarize, we have presented three metrics for robustness assessment (flow robustness, routing cost and network efficiency) and three metrics for resilience assessment (path redundancy, path disparity and node criticality). In the following section, we demonstrate the relevance of this selection of metrics to thoroughly characterize the dynamics of packet transmission and the reliability of the available paths in the network.

4. Impact analysis of graph division: application to nanosatellite swarms

In this section, we present a practical application of the theoretical approach described above. We focus on a nanosatellite swarm deployed in orbit around the Moon to perform space observations by analyzing very low frequencies. We prove in Sec. 4.4 that fair graph division makes a non-trivial improvement in the robustness and resilience of such a system.

4.1. Context of the operation

The study of Dark Age signals is a key research topic for understanding the early days of the universe and the formation of stars (Brown and Novaco (1978)). These signals consist of very low-frequency interferences, typically below 10 MHz. Unfortunately, they are hardly observable by current ground-based interferometers because of ionospheric distortion and Radio Frequency Interferences (RFI). One solution to alleviate this issue is to deploy a swarm of nanosatellites directly into space, as presented in the Nanosatellites for a Radio Interferometer Observatory in Space study (NOIRE) carried out by Cecconi et al. (2018). This study proves that the deployment of a nanosatellite swarm in orbit around the Moon is a viable solution for space observations of Dark Age signals while being protected from the Earth's RFI.

To be considered a valid space radiotelescope, the nanosatellite swarm must operate similarly to ground-based telescopes. There are four main stages in the process:

1. while on the dark side of the Moon, *i.e.* when the swarm is shielded from the RFI, each nanosatellite collects raw observation data from space;
2. each nanosatellite shares its data with each other member of the swarm and receives their data in return;

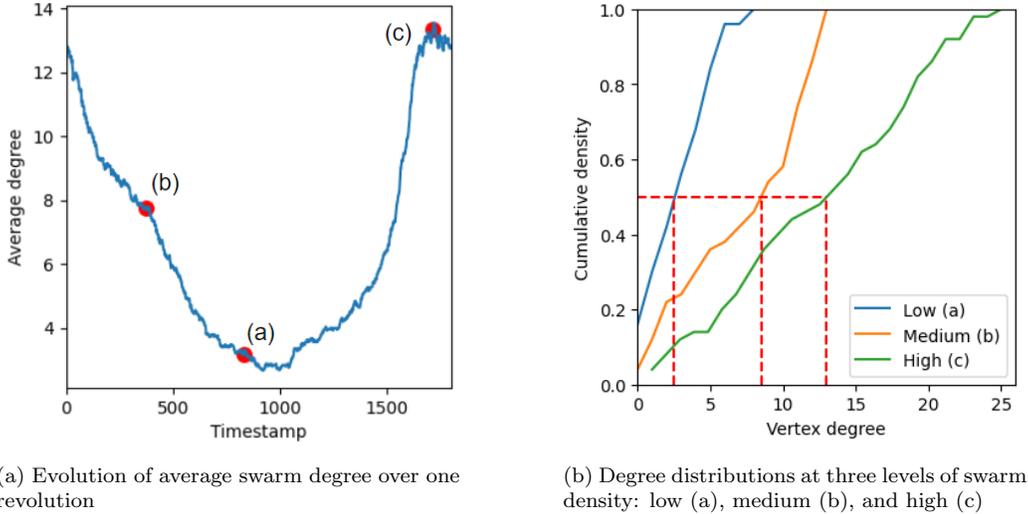


Figure 2: Estimation of swarm density: analysis of degree

3. each nanosatellite computes a cross-correlation matrix from all available data to produce a global interferometry image of space;
4. the swarm finally uplinks the image to a base station on Earth, preferably when the swarm-to-Earth distance is minimal.

It is primordial for such a system to be robust and resilient to perform its mission for the longest time possible.

4.2. Description of the dataset

We use nanosatellite position data generated synthetically using a Matlab simulator (Paimblanc and Mailhes (2018)). We consider a swarm of 50 nanosatellites orbiting the Moon. The dataset provides the positions of each nanosatellite of the swarm and their trajectory over time. There is no bootstrap stage, so the behavior of the swarm is stable over time.

The data consist of the (x, y, z) coordinates of each nanosatellite in the Moon-centered coordinate system, sampled every 10 seconds over a complete duration of 24 hours. The swarm performs a revolution around the Moon in 5 hours. The behavior of the swarm is quasi-identical for each revolution, so we choose to analyze only one period of revolution for simplicity.

During a revolution, the topology of the swarm evolves, particularly in terms of nanosatellite density. Fig. 2a shows the temporal evolution of the

average degree of the swarm, and Fig. 2b displays a close-up of the degree distribution in the swarm at three typical levels of density: a low-density topology, represented by a low average degree (point *a*), a medium-density topology, represented by a medium average degree (point *b*), and a high-density topology, represented by a high average degree (point *c*). When the density is low, around 20% of vertices are isolated and 50% have less than 3 neighbors. When the density is medium, some vertices are still isolated but 50% of vertices have at least 8 neighbors. Finally, when the density is high, there are no more isolated vertices and 50% of them have over 13 neighbors. Tab. 1 summarizes the properties of each topology.

Density	Low (a)	Medium (b)	High (c)
Number of vertices	50	50	50
Number of edges	80.6	217.5	325.5
Average degree	3.2	8.7	13
Number of connected components	8.8	4.2	2.3

Table 1: Topology analysis at each density level: average values

The evaluation protocol of robustness and resilience metrics, presented in Sec. 4.3, is performed over the complete revolution as well as the three topology close-ups to fully grasp the characteristics of robustness and resilience in the swarm.

4.3. Evaluation protocol

To understand the influence of fair graph division on the robustness and resilience of the network, we compute the robustness metrics (flow robustness, routing cost and network efficiency) and resilience metrics (path redundancy, path disparity and node criticality) on the original undivided graph. To do so, we compute these metrics at each timestamp over a complete revolution (we remind that the data are sampled every 10 seconds). Then, we analyze their distribution on each of the three levels of swarm density. These results represent the reference performance of the network in terms of robustness and resilience.

Then, we perform graph division with the chosen algorithm (RND, MIRW or FFD) in the initial phase of the swarm (*i.e.*, at timestamp 0), and fix the groups for the rest of the simulation so that the vertices cannot change groups

during the simulation. The results presented below are based on a graph division into 10 groups because this is the optimal number of groups to minimize the routing cost. We proceed to compute robustness and resilience metrics on the divided graph, similarly to the original graph. Because the proposed algorithms are based on random mechanisms, this operation (division and computation) is independently repeated 30 times to obtain a good estimation of the behavior of the divided graph. These results are then compared with the reference results of the original graph to highlight the impact of graph division on the robustness and resilience of the swarm.

4.4. Results

We analyze the performance of each algorithm on two aspects: the temporal evolution of the metrics, and the distribution of metrics values at three typical levels of network density (low, medium and high), as presented in Sec. 4.2.

Fig. 3 and Fig. 4 show the impact of graph division on robustness and resilience by presenting four cases: original graph (undivided), graph divided by RND, graph divided by MIRW, and graph divided by FFD. The figures in the left column represent the temporal evolution of the metrics. Each point of the curves symbolizes the value of the metric at a given timestamp. The figures in the right column show various boxplots for each case (original, RND, MIRW and FFD) and for each level of network density (low, medium and high). Each boxplot represents the values distribution of a given metric at a given level of network density. Note that the temporal evolution of the routing cost, depicted in Fig. 3c, has two y-axes because the routing cost of the original graph is much higher than that of the divided graphs. Likewise, Fig. 3d does not display the values distribution of the original graph because it is on a much higher scale and thus not relevant for comparison.

4.4.1. Reference results

Tab. 2 shows the cross-correlation matrix of the robustness and resilience results obtained from the original graph. Regarding robustness metrics (upper left box), there is a strong correlation between flow robustness and network efficiency: increasing one increases the other. Regarding resilience metrics (lower right box), there is a strong correlation between path redundancy and path disparity, which is expected from their definition in Sec. 3. We can also notice a few cross-correlations between robustness and resilience metrics (upper right box): flow robustness and network efficiency are strongly

Metric	$F(G)$	$R(G)$	$\Theta(G)$	$\Psi(G)$	$\Delta(G)$	$ C(G) $
$F(G)$	1	0.53	0.89	0.64	0.81	0.1
$R(G)$		1	0.12	0.15	0.11	0.8
$\Theta(G)$			1	0.69	0.9	-0.31
$\Psi(G)$				1	0.8	-0.11
$\Delta(G)$					1	-0.21
$ C(G) $						1

Table 2: Cross-correlation of robustness and resilience metrics based on the results of the undivided graph

correlated with path disparity, which implies that any modification to one of these metrics has the same impact on the other two.

The routing cost and critical set size are particular cases because the objective is to minimize these metrics. First, the routing cost is strongly correlated to the critical set size, which means that a reduction in the number of critical vertices also decreases the number of packets to transmit, and conversely. Although the other metrics are not strongly correlated to the critical set size, we can notice that increasing the network efficiency leads to a decrease in the critical set size, hence has a positive impact on the minimization of the number of critical vertices.

On the other hand, increasing flow robustness can lead to a non-trivial increase in routing cost. This negative impact is related to our packet propagation model: when a destination vertex is unreachable (*i.e.*, there is no path connecting to it), no packets are sent, so a poorly connected graph tends to have a lower routing cost. This bias can be compensated by forcing the graph to be connected by adding weighted edges between distant vertices. In this way, a path will always be available, but the transmission will possibly cost more. In this case, we would work with a weighted graph, but this is beyond the scope of this paper.

4.4.2. Results on robustness

Fig. 3 depicts the results on robustness and shows that each division algorithm has a positive impact on robustness over time and at any level of network density. The biggest gain is obtained on the routing cost (Fig. 3c), where each algorithm divides by almost ten the number of packets to transmit in the network. We can see in Fig. 3d that MIRW gets the lowest routing cost

independent of network density, in contrast to FFD, which gets the highest routing cost. The flow robustness also increases after division. Fig. 3a shows that MIRW and FFD perform better than RND, and increase flow robustness the most when the network density is low (Fig. 3b). Finally, regarding the network efficiency, Fig. 3e and Fig. 3f show that only MIRW and FFD are able to make an improvement, and more significantly when the network density is either low or high.

4.4.3. Results on resilience

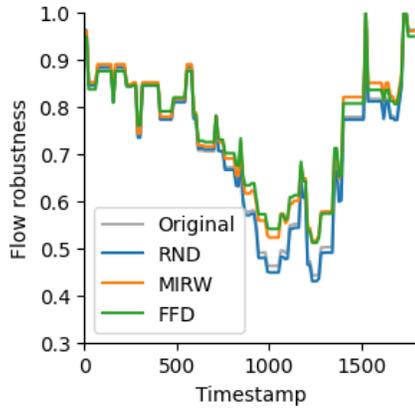
The results for resilience are globally more balanced than those for robustness. Fig. 4 shows that none of the algorithms can improve all resilience metrics simultaneously. The only improvement performed by MIRW and FFD concerns the size of the critical set, as shown in Fig. 4e and Fig. 4f. We can clearly notice a reduction in the number of critical vertices, although MIRW performs slightly better than FFD regardless of the network density. RND brings few to zero changes in the presence of critical vertices. The results obtained for path redundancy and disparity are related to each other, which is expected because they are strongly correlated. Fig. 4a and Fig. 4b show that RND is the only algorithm that does not decrease the path redundancy of the original network. MIRW and FFD decrease the path redundancy level the most when the network density is high: when the density is low, there is little difference between the algorithms. A very similar observation is made on the path disparity presented in Fig. 4c and Fig. 4d. However, it is important to highlight that MIRW and FFD do not decrease the path redundancy and disparity to extremely low levels either: depending on the application, such levels of path redundancy and disparity can be acceptable.

5. Related work

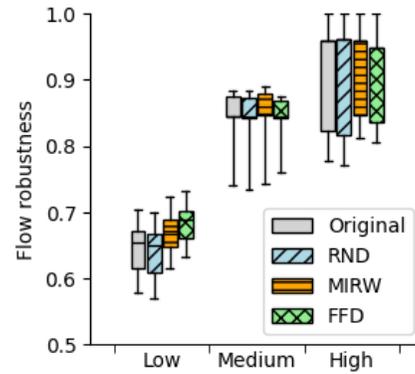
This section presents a compilation of studies relevant to the proposed investigation. We have categorized this state-of-the-art review into two segments: the first focuses on robustness, followed by the resilience aspect.

5.1. Robustness

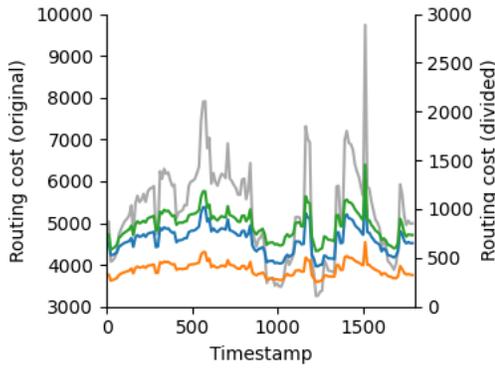
The robustness of a network characterizes its ability to maintain functionality and withstand internal and external faults. Achieving a high level of robustness is essential for countering intentional attacks and ensuring operation in hostile environments. Energy efficiency is a crucial metric for



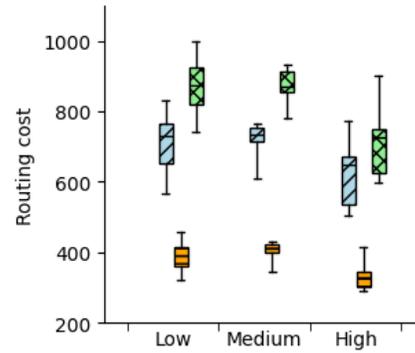
(a) Flow robustness (temporal)



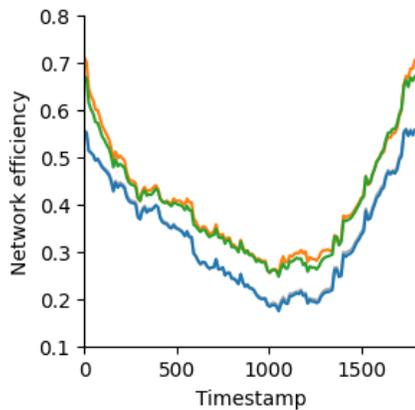
(b) Flow robustness (distribution)



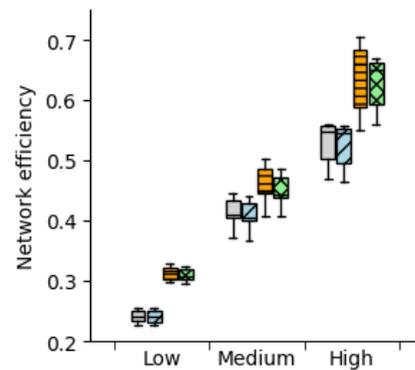
(c) Routing cost (temporal)



(d) Routing cost (distribution)

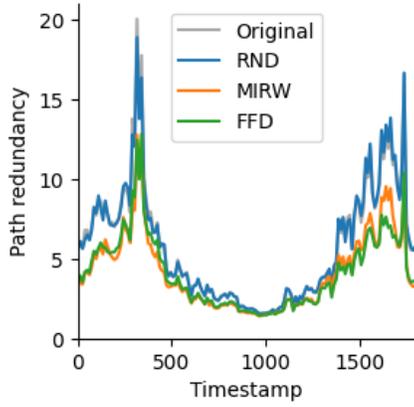


(e) Network efficiency (temporal)

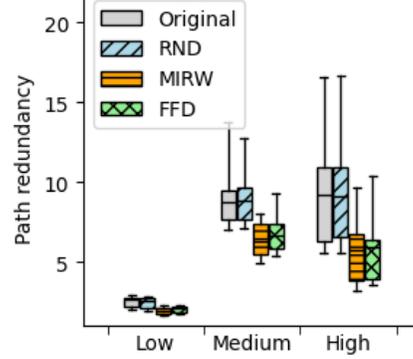


(f) Network efficiency (distribution)

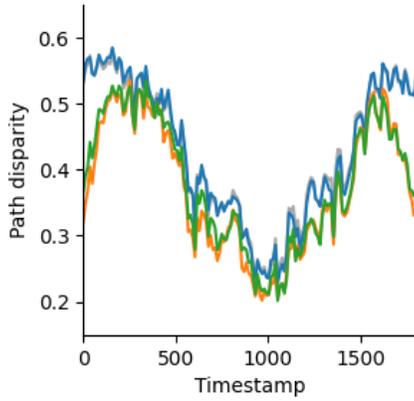
Figure 3: Temporal evolution of robustness metrics (left) and their distributions at three levels of network density (right)



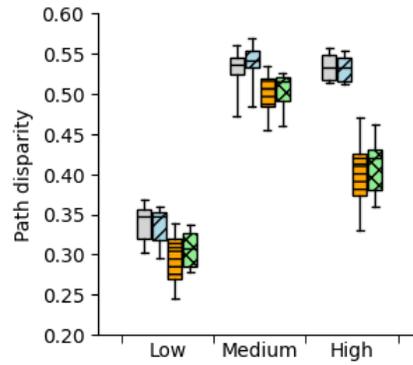
(a) Path redundancy (temporal)



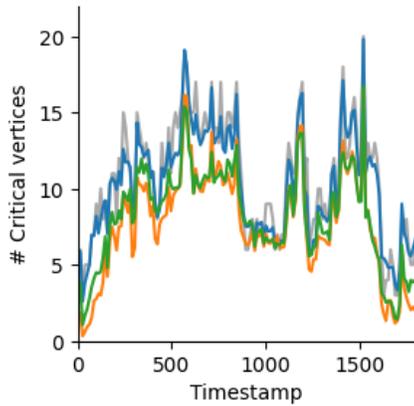
(b) Path redundancy (distribution)



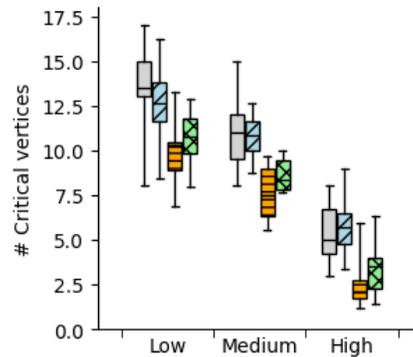
(c) Path disparity (temporal)



(d) Path disparity (distribution)



(e) Critical set size (temporal)



(f) Critical set size (distribution)

Figure 4: Temporal evolution of resilience metrics (left) and their distributions at three levels of network density (right)

robustness, particularly in Wireless Sensor Networks (WSN), where routing protocols play a vital role in finding optimal routes while considering energy consumption. Hierarchical protocols such as Low Energy Adaptive Clustering Hierarchy (LEACH) enhance the overall efficiency of WSNs, increasing network lifetime. A comparative analysis by Daanoune et al. (2021) evaluates 27 routing protocols derived from LEACH, considering metrics such as scalability, energy efficiency, and communication method. Although each algorithm has its strengths and weaknesses, they collectively contribute to improved network load balancing and reduce energy consumption, enhancing overall robustness. Identifying critical nodes is another crucial aspect of building a robust network. Liu et al. (2019) propose an algorithm based on weighted betweenness centrality to pinpoint central nodes in complex transportation networks. Identifying these major nodes is crucial for network safety and reliability. The authors demonstrate the accuracy of the algorithm in identifying critical nodes efficiently, with results consistent with real-world scenarios. Examining the impact of attacks on MANETs, Zhang et al. (2013) focus on the targeted attack scenario in which the highest-centrality nodes are affected in dynamic graphs of varying density levels. The authors establish betweenness centrality as a precise measure of node importance in highly connected graphs. However, in sparsely connected graphs, node degree and eigenvector centrality emerge as more accurate metrics for node significance. In the context of robust networks, ensuring a strong Quality of Service (QoS) is paramount. Marydasan and Nadarajan (2022) propose the Reliable and Stable Topological Change Adaptive Ad-hoc On-demand Multipath Distance Vector (RSTA-AOMDV) routing protocol to maintain QoS during data transmission. This protocol considers the local information of nodes while forwarding packets, resulting in superior performance in terms of Packet Delivery Ratio (PDR), throughput, and packet transmission time compared to traditional routing protocols such as AOMDV-MCA or SR-MQMR.

5.2. Resilience

The resilience of a network refers to its ability to recover from faults when they occur. The extensive literature on system resilience and sustainability spans various domains, including communication networks (referenced in Rak and Hutchison (2020)), transportation networks (referenced in Sun et al. (2020)), environmental sustainability (referenced in Sarkis and Zhu (2018)), and socio-ecological systems (referenced in Biggs et al. (2015)). Despite

differences across these domains, the definitions of resilience and the measurement methods remain consistent. The Internet serves as an example of a communication network with low resilience. Sterbenz et al. (2010) introduce an architectural framework that enhances communication network resilience by incorporating resilience strategies and principles into the analysis. The authors underscore the importance of considering resilience in communication network design. In complex networks, Kharrazi et al. (2020) present metrics for evaluating resilience, particularly in resource trade networks. Their evaluation involves statistically characterizing resilience through redundancy (the number of duplicate elements), diversity (variety, distribution, and disparity of elements), and modularity (a system’s capacity to fragment into distinct communities to contain shocks or stress). For MANETs, Ladas et al. (2016) propose the Multipath-ChaMeLeon (M-CML) resilient routing protocol. M-CML, based on a multipath approach, reduces end-to-end delay and improves the PDR compared to the Optimized Link State Protocol (OLSR), albeit with a higher number of redundant packets. Resilience in MANETs also plays a crucial role in disaster management. Molla et al. (2019) introduce a hybrid Wireless Multi-Hop Network (WMHN) architecture, combining Flying Mesh Networks (FMN) and opportunistic MANETs to enhance connectivity with survivors, reduce packet loss, and decrease end-to-end delay. To evaluate the resilience of public transportation networks, Jing et al. (2019) assesses the number and availability of alternative paths. A resilient transportation network, defined by extensive route redundancy, is characterized by efficient and reasonably short alternative paths that consider travel costs. In addition, the authors evaluate the connectivity and accessibility of the studied metro networks.

Our position in this literature review is to analyze the impact of a given mechanism and/or algorithm (in our case, graph division) on both robustness and resilience. We consider that these two properties should not be studied separately because they have a mutual influence on each other. Hence, we propose a general methodology to combine the assessment of robustness and resilience levels in MANETs. This methodology can be a great help for researchers conducting comprehensive studies of robustness and resilience levels in complex systems.

6. Conclusion and future research

Optimization of robustness and resilience is crucial in Mobile Ad Hoc Networks (MANETs). A robust network withstands internal and external faults, while a resilient network maintains functionality despite faults. This study focuses on enhancing the robustness and resilience of MANETs, which are treated as temporal graphs, through network architecture optimization. Our approach involves graph division by assigning each vertex to a group without isolating them. We examine the impact of random selection algorithms (RND) and exploration algorithms (MIRW and FFD) on the original graph by analyzing flow robustness, routing cost, network efficiency, path redundancy, path disparity, and node criticality. Applying this evaluation protocol to a practical application—a nanosatellite swarm orbiting the Moon acting as a distributed radio-telescope—, we demonstrate that random selection and exploration algorithms significantly improve system robustness by reducing routing costs. Notably, MIRW outperforms FFD and RND in reducing routing costs. Exploration algorithms, overall, excel in robustness optimization compared with random selection algorithms. With respect to network resilience, exploration algorithms decrease the number of critical vertices but also decrease path redundancy and disparity. Random selection algorithms neither improve nor reduce resilience. In conclusion, graph division positively impacts MANETs’ robustness and resilience. Exploration algorithms enhance robustness but affect specific resilience metrics, whereas random selection algorithms are practical for robustness optimization.

Future research should explore the impact of a time-varying number of vertices in the graph, considering additions and deletions over time. Our work assumes a faultless model with a constant number of vertices and aims to investigate weighted graphs, where the data transmission cost depends on the distance between MANET nodes. This scenario is crucial, considering each node’s ability to contact others while considering transmission cost.

Acknowledgements

The authors would like to thank the CNES and the TéSA laboratory for supporting their work.

References

- Akopyan, E., Dhaou, R., Lochin, E., Pontet, B., Sombrin, J., 2023. Fair network division of nano-satellite swarms. 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) , 1–5.
- Alyassi, R., Khonji, M., Karapetyan, A., Chau, S.C.K., Elbassioni, K., Tseng, C.M., 2023. Autonomous recharging and flight mission planning for battery-operated autonomous drones. IEEE Transactions on Automation Science and Engineering 20 (2), 1034–1046.
- Biggs, R., Schluter, M., Schoon, M.L., 2015. Principles for building resilience: sustaining ecosystem services in social-ecological systems. Cambridge University Press.
- Brown, L., Novaco, J.C., 1978. Non thermal galactic emission below 10 mhz. The Astrophysical Journal .
- Cecconi, B., Dekkali, M., Briand, C., et al., 2018. Noire study report: towards a low frequency radio interferometer in space. 2018 IEEE Aerospace Conference , 1–19.
- Daanoune, I., Abdennaceur, B., Ballouk, A., 2021. A comprehensive survey on leach-based clustering routing protocols in wireless sensor networks. Ad Hoc Networks 114, 102409.
- Jing, W., Xu, X., Pu, Y., 2019. Route redundancy-based network topology measure of metro networks. Journal of Advanced Transportation 2019.
- Kharrazi, A., Yu, Y., Jacob, A., Vora, N., Fath, B.D., 2020. Redundancy, diversity, and modularity in network resilience: applications for international trade and implications for public policies. Current Research in Environmental Sustainability 2, 100006.
- Ladas, A., Pavlatos, N., Weerasinghe, N., Politis, C., 2016. Multipath routing approach to enhance resiliency and scalability in ad-hoc networks. 2016 IEEE International Conference on Communications (ICC) , 1–6.
- Liu, W., Li, X., Liu, T., Liu, B., 2019. Approximating betweenness centrality to identify key nodes in a weighted urban complex transportation network. Journal of Advanced Transportation .

- Marydasan, B.P., Nadarajan, R., 2022. Topology change aware on demand routing protocol for improving reliability and stability of manet. *International journal of intelligent engineering and systems* 15.
- Molla, D.M., Badis, H., Desta, A.A., George, L., Berbineau, M., 2019. Sdr-based reliable and resilient wireless network for disaster rescue operations. *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)* , 1–7.
- Paimblanc, P., Mailhes, C., 2018. Définition d’un référentiel spatio-temporel autonome dans une constellation de satellites. *Technical Report. CNES - TéSA*.
- Rajan, M.A., Chandra, M.G., Reddy, L.C., Hiremath, P., 2008. Concepts of graph theory relevant to ad-hoc networks. *International Journal of Computers, Communications and Control* 3, 465–469.
- Rak, J., Hutchison, D.e., 2020. *Guide to disaster-resilient communication networks*. Springer Nature.
- Robinson, Y.H., Krishnan, R.S., Julie, E.G., Kumar, R., Son, L.H., Thong, P.H., 2019. Neighbor knowledge-based rebroadcast algorithm for minimizing the routing overhead in mobile ad-hoc networks. *Ad Hoc Networks* 93, 101896.
- Sarkis, J., Zhu, Q., 2018. Environmental sustainability and production: taking the road less travelled. *International Journal of Production research* , 743–759.
- Sterbenz, J.P., Hutchinson, D., Cetinkaya, E.K., Jabbar, A., Rohrer, J.P., Scholler, M., Smith, P., 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks* , 1245–1265.
- Sun, W., Bocchini, P., Davidson, B.D., 2020. Resilience metrics and measurement methods for transportation infrastructure: the state of the art. *Sustainable and Resilient Infrastructure* , 168–199.
- Zhang, D., Cetinkaya, E.K., Sterbenz, J.P., 2013. Robustness of mobile ad hoc networks under centrality-based attacks. *2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)* , 229–235.